

Control Lost
Tech going loose

Contents

1- Losing Control over data

2- Humans Losing Control: AI/ML/IOT

3- Losing Control over Crimes: Digital crimes. Data leaks. Cyberattacks and vulnerabilities. Bullying. Identity Thefts

4- Losing Control over Work: Stress and Loss of Control at Work. Working remotely. Technology overload. Consumer Support. Sorry, it's the computer system. Can't do anything. Disruption: Publishing, Media, Legal, Finance : Cryptocurrencies, Airlines, Transportation, Healthcare .

5- Losing Control inside *Tech*: Amazon vs. Elastic Search. Technology evolves rapidly. Graphic Design vs. User Experience vs. Javascript. Engineering, Open Source , Hacking, Code of Conduct. Inadequate Job Hiring profiles. Role of algorithms and data structures. No No No: NoCode, NoSQL. The Language War/ Operating System War. Is it still relevant? - Tableau, Miro, Airtable, Notion, Zoom, etc. The new business models. Where have IBM and Microsoft gone? Platforms. Frontend, Databases, Frameworks. The role of Facebook, Google, Twitter, Uber

6- US Losing Control: Innovation: Where? US: Silicon Valley, Investments (> 1B\$ in California, otherwise woman of color owned business), and Government-funded Research. Internationalization, Outsourcing and Immigration: India, Ukraine, Rumania, China. Europe and Regulations. US Government Losing Control: How to make it work from inside tech. Passive Government. Congress and Technology. Government ought to do something. NIT.

7- Remedy: NIT

Feeling of inevitability, immutability, immunity
Rules of SEO similar and multiple checking comparable to tax return constraints.
Notion of net states vs nation states (Alexis Wichowski)
Feeling of powerlessness.

File - /Users/michel/Documents/work/books-articles/book2021/toword

```
pandoc --wrap=none -s toc.md -t docx -o word/toc.docx
pandoc --wrap=none -s chapter1.md -t docx -o word/
chapter1.docx
pandoc --wrap=none -s chapter2.md -t docx -o word/
chapter2.docx
pandoc --wrap=none -s chapter3.md -t docx -o word/
chapter3.docx
pandoc --wrap=none -s chapter4.md -t docx -o word/
chapter4.docx
pandoc --wrap=none -s chapter5.md -t docx -o word/
chapter5.docx
pandoc --wrap=none -s chapter6.md -t docx -o word/
chapter6.docx
pandoc --wrap=none -s chapter7.md -t docx -o word/
chapter7.docx
pandoc --wrap=none -s techbio.md -t docx -o word/techbio
.docx
```

Book2021

File - /Users/michel/Documents/work/books-articles/book2021/.gitignore

```
/.idea/  
/pdf/  
/word/  
/sources/  
/archive/  
.DS_Store
```

1977-78 Publishing

I started my career as a science book editor at Hachette . I was responsible for publishing science text books and was covering the whole process: getting the manuscripts out of the authors, proofreading, layout, graphical mockup, dealing with illustrations, with graphic designers and photographers, organizing the project with multiple players, getting involved in the pre-press preparation project, designing the pages, tweaking the layout, reviewing the book, ordering and choosing the book cover, sending the books to the printer, and following up with the sales department on directing them on the highlights of particular books. This work was covering many aspects and I enjoyed doing it.

A couple of years later, I was offered the opportunity of a fellowship to do a PhD on Albert Einstein as several events were planned for its centennial in 1979, and it was an opportunity to complete my academic credentials. I accepted to leave my work (which may have been the biggest mistake of my whole professional life, but I couldn't possibly know at the time).

1979. First Personal computers

I started programming in BASIC on a TS 80 Model 3 in 1979 and on an Apple 2. Programs were then saved on a cassette that was not always readable. I often had to retype the whole program after failing in several attempts to read from the tape. The first programs I created were part of my PhD work on a public presentation of Albert Einstein's life and work. The computers were eventually placed in museums to be used by the public: the Library of the Pompidou Center and the scientific museum Palais de la Découverte in Paris.

1982 Incompatible Floppy Disks

My second programming experience consisting in building a database system for managing inventory and sales for a family owned clothing store. I used an IBM PC that was located in the house of a friend of my father who was working for IBM and had a computer in his home that he was not using during the day. I had to schedule the shifts with his son, who was also using the same computer. This computer has floppy disks. However, the client for whom I was creating this software, who was located 150 miles away, had purchased another computer,

Sirius, which was also using MS-DOS but was not able to read the same floppy disks that were created on a IBM PC . Therefore, each time I went there, I had to retype the whole program by hand. It was working the same way, apart from some subtle differences that needed attention (I don't remember the details).

1983-1989 Word processing adventures

I spent years working as a freelancer in science magazines, and translating books for publishers in history, philosophy and sociology of science. I was spending most of my time writing. I started by using a typewriter, as this was the only affordable at that time , but quickly found out that there were other solutions available.

My first own computer was a laptop: the TRS 80 Model 100 . It was a fantastic progress as my main work was translating books, and I used a typewriter. For the first time, I was able to type the book on the computer and edit it. I was using the built-in word processor, which showed 8 lines of text on an LCD screen, and I could use the arrow keys and delete keys to browse into the text and correct it. I managed to connect the daisy-wheel typewriter and had to fill the pages one by one to be printed, but that was a great progress compared to what I used before. However, because I was using French, the support for accented characters was not great, because if I used the built-in encoding, the result was different from what I expected. I learned to program in assembly language for this machine and wrote some tools to automatically translate the text by changing the accented characters into characters that were compatible with the typewriter. I helped other people who had the same problem.

A couple of years later, I won a lottery at a professional fare and got an Epson PX8 laptop, which was slightly better than the TRS-80 because it used CP/M, which was an operating system with more functionalities than the built-in proprietary system for the TRS-80, and it had a built-in micro-cassette system that was more reliable than the tape-recorder used with the TRS-80 model 100. Moreover, it contained the word processor that was gaining traction at that time, WordStar. WordStar was more complicated to use than the one I was using before, but it had support for bold, italic characters, and the like.

When I got involved with the US-based project aimed at the publication of Einstein papers, first located at Boston University, later at Princeton University, I was exposed to WordPerfect, and the person who introduced me to it was very enthusiastic about it. I could see immediately that this was much more powerful than anything I have been using before, and became a WordPerfect addict. As I was trying to organize the data around the book in a database, I started to dive into the macro language and designed ways to automatically insert data from the database into the text. I built a system that allowed me to dynamically work on the database part as well as on the text and to use macro-driven merge facilities to produce the text I needed.

I became an instructor for WordPerfect-France and started to teach courses on their macro-language for their advanced users. I was also at that time starting to teach secretaries how to transition from typewriters to word processing.

As printing was shifting from lead type technologies to phototypesetting, I learned that the National Association of Publishers in France was interested in transitioning to computer-assisted techniques, and attended presentations on a new language that represented the future of publishing: SGML (the Standard Generalized Markup Language) was pushed by a handful of technical enthusiasts whom I met, and told them that I was interested to join them. I was offered the gig of translating the standard into French for the French National Standards Association (Afnor).

1989 Electronic Documents for Engineers

In 1989, I was contacted by an engineering school which was looking to replace the head of their Department "Scientific and Industrial Communication" and interviewed me about which orientation this department could take. I first said that I didn't what the word "communication" means in this context. If it was about organizing events, I was not the right person to discuss to, as I had no experience, not was I interested, in organizing events. I was asked whether scientific journalism history of science was a possible option, to which I answered that it was probably a good minor to have as it opened minds of future engineers. However, I said, there is a new domain that is gaining traction and is potentially an engineering domain: electronic document management, as it was called at the time, and I

mentioned SGML as one new technological foundation that was changing ways that the printing production chain was working on.

The curriculum I created included standards, technical documentation, image processing, hypermedia. I hired the industry leaders and consultants, frequent speakers in professional conferences, and I attended their presentations. I learned as much as my students, and could see where technology was heading. The students had no problem finding internships and later jobs, as the industry was looking for profiles of people who were exposed to those emerging technologies and had an engineering profile.

I was invited one day to attend a presentation organized by IBM. The speaker was Charles Goldfarb, the father of SGML, himself working for IBM at that time. He started by saying that he wouldn't speak about SGML, because that was the past, but instead would be speaking about the future, a new hypermedia language in the making, called HyTime, an acronym for Hypermedia Time-Based Structuring Language. And his presentation was based on slides that contained images of people in cars, in American grid-structured cities, synchronizing their position in time and space using light signals. He also said that only 10 people in the world understood HyTime.

His presentation was a shock for me: During my doctoral work about the reception of the theory of relativity, I studied Einstein's description of space-time illustrated by synchronizations of frames of references using light signals. I also studied various facets of the Einstein celebrity including the statement that only ten people in the world understood Einstein. I couldn't help not seeing the parallels. After Charles Goldfarb ended his talk, I went to talk to him and asked him whether he used the special relativity theory as a foundation of the HyTime model. He answered: I am a lawyer, the slides were actually produced by a musician who contributed to HyTime, we have no scientific background, but we'd be glad to know whether what we are doing have any resemblance with existing scientific work. I encourage you to look into this and let us know what you think.

1992: How the Web started

A few days later, while sitting in my office at the university, I received a phone call from the National Research Agency (Ministère de la Recherche), which had

previously founded a study I did about the introduction of SGML in the publishing industry. We liked your study, we have some funds available that we need to spend before the end of the fiscal year. If you are able to give me a theme for a project during this phone call, you could have it. I thought about for a few seconds, and replied. What about studying the relationship between HyTime and Einstein. He asked: what is HyTime? I answered: The successor of SGML. He said: you got it! An SGML conference was planned in the spring of 1992 in Amsterdam. There was still time to submit a proposal for a paper. I sent a proposal about comparing the HyTime model with Einstein's special theory of relativity, and the proposal was accepted. Then I started to panic. I received the material about HyTime by mail (at that time, paper was still the dominant way to get documents). I understood why only ten people could understand it. At least, I understood I was definitely not one of them. The only way forward was to get acquainted with the members of the HyTime team, and to interview them to try to understand what they were trying to do. At the same time, I started to draft a 2 column table in which I compared the principles of the special theory of relativity with concepts used in HyTime.

I used the funds I got for this research to attend an international standards meeting in Copenhagen, where HyTime was discussed. This was a one week meeting, which was scheduled just before the conference in Amsterdam. When I arrived, I learned that the HyTime team had just spent the preceding week working non-stop, days and nights, and they announced they were ready to go for publication. It was too late for me to discuss my findings, or even questions, about the relation with a scientific theory. They were exhausted but happy about the work being completed. I started to discuss with the co-author of HyTime, the musician who created the slides on synchronizing positions in time and space, Steven Newcomb, who was glad to find someone that was interested and eager to learn. He explained to me what it was about. The story was quite fascinating.

Before HyTime, there has been an attempt to develop a generic language for music notation, that encompasses not only traditional western notation on scores, but also other music styles, with a different internal structure. The project was not only about simply describing music, but also its rendition, i.e. the way it was staged during representations, operas. There were provisions to describe the ways that a director could

design the way performances should be interpreted. The model was incorporating into HyTime as the scheduling and rendition modules. In addition, HyTime contained a location module, enabling to describe how every data points can be represented in relation to others, and a hypermedia module, featuring various models for links incorporating the notions of aggregates, directionality, traversals.

SGML got a big boost when the US DOD made a requirement that all its suppliers should provide all their information in this format. The DOD also played an important role promoting HyTime. When they first heard about the music standard, they told the members of the working group that they should get rid of anything purely musical, instead describe the generic ways to stage scenes in order for them to be able to use it to describe military operations, and add hyperlinking facilities, as hyperlinking was an important and hot issue at that time. That's how HyTime was born.

At the same time, work was going on a simple hypermedia language that can be used on the Internet, using the same notations as SGML, while releasing many of the constraints that SGML documents were supposed to follow.

The Hypertext Markup Language, aka HTML, was created to be usable with a protocol called http (Hypertext Transfer Protocol). These new products constituted the foundation of the World Wide Web, which was launched in 1993.

HyTime was indeed very complex and very rich. It contained many breakthroughs, and many of them started to become the sources for independent developments and new standards.

The location module gave rise to the Document Object Model (DOM) which is the common technology used by the Web browser to retrieve and display data. It also gave rise to the XPath standard, that is used to express how things are located. I was more interested in the Hyperlink module.

Starting in 1991, a study group which started among various Unix vendors was working on ways to make the documentation of the various flavors of Unix more consistent. Different terms were used for the same thing by different vendors. At that time, Unix was used for serious computing, and was the operating system for most workstations. Sun, Hewlett-Packard, Digital were among

the companies that provided Unix product. That was also the time where Linux started, as a free, open-sourced, disruptive flavor of Unix.

Losing Control over Data

1. Overwhelmed by data

Our societies get many benefits from technology, but technology brings also negative side effects. This book is about finding where the dark side of technology resides, analyze the effects and discuss how to alleviate them.

Data is everywhere and rules the world. There is so much of it that automated processes to extract and process data has become essential. The expression "Artificial intelligence" is used to describe those processes, and the term serves also for his proponents to claim that machines are superior to humans. Consequently, the social status of "knowledge workers" is being downgraded. The irony is that the traditional progressive view is based on the belief will make human labor less painful, and the reality is that although this is happening, at the same time, work has becoming more dull, less creative, and individual initiatives are drastically limited because of the dependency to technology. This generates a feeling of uselessness.

Technology is complex, and technological products are very complicated constructions made to enhance the user experience. However, most often than not, users don't really have their say in the design of the applications. The perverse consequence of this is that the user must learn to behave as they were satisfied, whether that's true or not. Instead of being in the driver seat and express requirements that translate into a product that corresponds to their needs, users should lower their expectations to fit the actual limitations of the software they use. The term "user" says it all. The power is in the hands of the technology providers, not their users. This generates passivity.

Information technologies generates all kinds of data, including tracking recordings. There is nothing that can not be traced and recorded: activities, locations, clicks, visited links. Companies record their employees usages of computers. Wearable devices, such as smartphones, record their location in a very precise manner, as well as date and times, and the wireless-enabled objects (refrigerators, beds, watches) report all kinds of data, including health reports containing the kind of information that is usually available in medical tests such as blood tests. The feeling of being

constantly monitored in all aspects of life generates a feeling of resignation and inevitability. It seems that the price to pay to use technology is accepting to give away anonymity and privacy. This generates initially a discomfort, that later becomes numbness or indifference.

If we can't avoid it, we are better off accepting it and ignore it.

Going online is like walking in a street. When we go out, we expect to be recognized in the street by our neighbors or acquaintances. If we want to stroll incognito, we we have to be creative and use a specific outfit designed for that purpose: for example, a combination of a burka, face mask and sunglasses. But that is not convenient nor socially acceptable way to behave. We are not supposed to hide when we are in an open space. This parallel helps us accept the fact that if we go online, we should not expect any privacy, since this is an open space.

However, things are not that simple. Scores of online activities need to be protected. For example, financial transactions on a bank account should not be open to the public. But, as in the street we run the risk to be hit by pickpockets, online we incur the risk to be hit by thieves who steal our online credentials to penetrate into our private sphere. Changing often passwords, using two or three step identifications are band aids that create more burden to the user, go a long way to protect us, but are in no way considered an absolute protection. If we are the victims of online attacks, the companies providing the services are often not considered liable, although there are exceptions.

Terms of service provided by online providers do not leave room for negotiation. These terms are unilateral and they can only be either accepted or refused. Disagreeing with some of the aspects of terms of service is not an option. Consequently, there is no real incentive in reading the fine print. This creates a sense of imbalance, and the recognition that corporations that provide services have the power to protect themselves, not us.

Credit scoring is a complex game invented by the financial institutions that rely on an average expected behavior. A good expected behavior does not consist in maintenance a healthy financial balance by having zero debt, but to manage debt in a way that both maximizes the profit for financial institutions, which charge

interest rates, and show overall that the beneficiary of credit services remains in control of the services they use. Any accident, even involuntary, or happening without the knowledge of the credit user, negatively impacts the credit score. Rebuilding credit is a long and painful road. Our online reputation on social media uses a similar model and establishes how much people appreciate what we are doing. Online reputation rewards contradictory things: how socially acceptable and mainstream we behave, or how much outrageous and dramatic we are. Inside technology, online reputation is connected to our usefulness in helping others. Hiring factors the online reputation as an essential factor. Between two candidates with an equivalent skill level, the one who has the most visible online presence and highest reputation will be selected.

Sharing applications use reputation. Uber or Lyft drivers, AirBnB hosts are rated. They also rate their customers. When using these applications, any record is being shared. This has the positive effect of encourage friendly behavior when using these services, but also generate some average conformant, expected, average behavior. Consequently, it is strongly discouraged to use any of these services when in a bad mood, or stressed situation, because the consequences of any incident can be long-lasting. When cars will be able to detect, through sentiment analysis, that a person is too stressed out to be able to drive a car, the car won't start. As some one objected during a conference presenting this issue, what if a person tries to escape by car from a criminal having penetrated into their house? Or if you are trying to rush to a hospital with a family member having a heart attack or a stroke?

China is using credit scoring and pushing it to a whole new level. Social credit scores measure how much an individual supports the actions of their government. People who have poor credit scores, either because they are offline or they refuse to play the game, are cut off from several services, and are prevented from certain essential services, like the ability to travel [^AW-China-Travel]. Friendliness, good reputation, conformance to social norms can gradually lead to obedience and servility in an authoritarian regime.

[^AW-China-Travel]:Alexis Wichowski, The Information Trade – How Big Tech Conquers Countries, Challenges Our Rights, and Transforms Our World, Harper Collins, 2020.

Loss of responsibility for content publishing makes rumors, fake news, political propaganda, technically indistinguishable from real, well-curated, respected source news, and it is practically impossible in practice believers that their sources are not to be trusted. The equality between truth and lies is poisoning the political atmosphere, creates extreme polarization and diminishes the credibility of any form of social contract, rights and duties, especially in democratic societies.

As everything we do is broadcast and reported, abuses happen also because of misinterpretation of what we do. A university professor who pronounces the N... word, even to analyze the way it has been historically used, is quoted having said it, and can be dismissed because of a clip taken out of context. The traceability results in people losing jobs.

Complete transparency, as provided by social media and made totally indestructible by Blockchain can be a good thing and at the same a bad thing. Restoring identity jeopardized by identity theft, escaping from bullying, getting on a no-fly list because of homonym situation, creates a feeling of despair.

Uselessness, indifference, passivity, despair, powerlessness, conformity, loss of common references, are among the side effects generated by technology. From there, it is tempting to consider that democracy is something from the past, and authoritarianism is the only viable solution for the future.

This resignation however negates two factors, that need to be analyzed, and could serve as a basis to fight against it.

1. Those who have vested interests in pursuing and aggravating the current trends know very well how to push it, they understand better what to do to extend their influence, and can do that without obstacles. It is important to understand how they operate, and find what can be done to limit their ability to expand their grip. What have they understand than others have not? Is optimism equivalent to naïveté?

2. Technology is not a black box that can't be opened. It's a universe populated by lots of people, who play very different roles, it's made of lots of layers, it has become complex enough that it's almost impossible to

grasp it into a single overall concept. When seen from inside, technology has many aspects. Many of those aspects are not hidden, they can be learned, studied, practiced. Many parts of technologies are open-sourced, and anybody who is curious can get acquainted with a piece of it.

This list contains 328 concepts, activities, domains, that are arbitrarily extracted from the domain of technology. Each of them is linked to a specific activity, with a specific set of approaches, tools, and perspectives that each support specific skill sets, and professional careers. This list is far from exhaustive, it has been created by looking mainly at the job offers in technology. Please note that this list doesn't contain any acronym nor any specific language or product, just concepts, methodologies, generic approaches and product types. It is only the tip of the iceberg of what technology is. However, many of the terms listed here have a direct impact on our daily lives, on the products we use. Here it is:

Access, Accuracy, Actionable insights, Agile, Algorithms, Application Programming Interface, Applications, Architecture, Artificial Intelligence, Assembly Language, Asynchronous, Attack, Audio, Auditing, Automation, Back End Development, Backend, Best practices, Big Data, Blockchain, Browser, Bugs, Business Intelligence, Business Value, Canvas, Cascading Style Sheets, Certification, Change Management, Channels, Chat, Client, Cloud, Cloud Development, Code Review, Coding, Collaboration, Commands, Commissioning, Components, Computer Science, Concept Maps, Confidentiality, Connected Applications, Connected Devices, Connections, Consulting, Containers, Continuous Deployment, Continuous Integration, Copyright, Credentials, Cross Site Forgery, Cross-functionality, Cryptocurrency, Cryptography, Customer Feedback, Customer Success, Cybercrimes, Cybersecurity, Dashboard, Data, Data Analysis, Data Bricks, Data Collection, Data Curation, Data Entry, Data Extraction, Data Governance, Data Ingestion, Data Integration, Data Lake, Data Loading, Data Models, Data Operations Analysis, Data Processing, Data Science, Data Scientists, Data Structures, Data Transformation, Data Typing, Data Warehouse, Data-driven solutions, DataOps, Databases, Decommissioning, Defect Analysis, Deliverable, Delivery, Deployment, Desktop, DevOps, Diagnostic, Digital Applications, Digitization, Directories, Discussion Group, Distributed Denial-of-Service Attack, Documentation, E-Commerce Platforms,

Extract-Transform-Load Pipelines, Elastic Search, Electronic Payment, Email, Encoding, End Users, Engineering, Enterprise Data Systems, Environment, Environment Variables, Evangelism, Face Recognition, Features, File, Files, Folders, Forensics, Format, Frame, Framework, Front End Development, Frontend, Full Stack, Full Stack Development, Functionalities, Garbage Collection, Geospatial Data, Global Network, Graph Database, Hacking, Handwriting Recognition, Hardware, Helpdesk, High Level Language, Hosting, Hypertext Markup Language, Information Technology, Information Technology Operations, Information Technology assets, Implementation, Industry Standard, Infinite Loops, Information architecture, Infrastructure, Instructions, Intellectual Property, Intelligent Analysis, Interfaces, Internet, Internet Service, Knowledge Graph, Knowledge Management, Knowledge Network, Languages, Laptop, Latency, Libraries, Linked Data, Local Storage, Logging, Login, Longitudinal dataset, Loops, Machine Learning, Maintenance, Maps, Mass mailing, Memory Leak, Messaging, Micro-services, Mind Maps, Mobile Apps, Mobile Apps, Mockup, Modeling, Modules, Natural Language Processing, Network, Network Engineering, Network Manager, NoCode, NoSQL, Object Database, Object Relation Mapper, Object-relational mapper, Office tools, Online ads, Open Source, Operating System, Operating System, Optimization, Orchestration, Organizers, Outages, Pair programming, Parallel processing, Penetration Testing, Performance, Phishing, Photo Editing, Pipeline, Platform as a Service, Platforms, Platforms, Port Scanning, Ports, Preventative Maintenance, Privacy, Problem Solving, Problem definition, Problem-solving, Procedures, Production, Production Systems, Programming, Programming languages, Project Management Software, Proprietary Software, Purple Teaming, Push / pull, Quality Assurance, Queries, Query languages, Rapid Development, Raw Data, Read-only access, Read-write access, Recommendation Engine, Relational Database, Representation of results, Resilient Technology, Reusability, Reverse Engineering, Robustness, Rollouts, Scaling, Schedulers, Schemas, Scientific Apps, Scientific Data, Scrum, Search Engine Optimization, Search Engines, Secrets, Security, Security, Semantic Web, Server, Service Deployment, Site Reliability, Slides, Smartphone, Social Media Platforms, Software, Software Development Lifecycle, Software as a Service, Sound Card, Specifications, Speed, Spreadsheet, Spreadsheets, Stakeholder Assistance, Standards, Startup, Statistical Analysis, Statistical modeling, Storage, Store Procedures, Streaming, Structured Data, Subject Matter Experts, Subscriptions,

Summary Reports, Support Libraries, Support Specialist, Surveillance, Synchronous, System Administration, System Architecture, System Functionality, System Security, System Design, Tables, Teamwork, Technical Issues, Technical Support, Test Automation, Test Cases, Test Reports, Test Scripts, Testing, Testing, Text Processing, Threats, Topic Maps, Touch Screens, Traceability Matrices, Tracking, Training, Troubleshooting, Trust, URL, Unstructured Data, Updates, Upgrades, Usage Guide, User Experience, User Guide, User Interaction, User Requirements, User-Friendliness, Validation, Variables, Video, Video call, Virtual Private Network, Virtual Reality, Viruses, Visualization, Voice Recognition, Voice recognition, Vulnerability Management, Web, Web Apps, Web Apps, Web Framework, Webinar, Workflow, Workstations

Time to dive in.

This book is not a general introduction to technology that aims at explaining all the aspects listed above. But it is an attempt to start breaking the glass ceiling by looking at technology in what it is essentially: a human activity, made by many people. Time has come to stop considering technology as a secret, magical, god-like, impenetrable black box against which no human action is possible. In other words, if technology is an ocean, it's time to learn to swim, to avoid getting drawn into it. Not just as "users", but as citizens who have rights, opinions, and want to stay in control of their lives.

Some of the obstacles are easy to overcome. As animals, humans tend to limit their territories by putting some unique signs preventing outsiders to get in. The technological community, as many corporations do also, has been prolifically using acronyms. Acronyms are the best way to exclude newcomers from getting in. For example, these are some randomly extracted from job ads in Big Data: AWS, SAS, JPM, MATLAB, SQL, R, CI/CD, GIT, JIRA, GPA, HDFS, ORC, T-SQL, MDX, DAX, NoSQL, MECE, ETL. Whatever each of them means, whether they are products, languages, processes or methodologies, they mean that if you don't know them, you don't belong to that community, you are not qualified in those technologies, and you don't have a chance to get a job before you learn at least some of them, not only what they mean, but how to operate them. But that's comparable to any corporate or institutional jargon that is acquired by

necessity. For example, 1040, 1099, W-2 are not just random numbers or combinations of letters and numbers. Anybody who is working or has worked in the United States understands that those numbers mean that, in order to file a tax return, you need to determine whether you have worked as an employee or an independent contractor and fill the appropriate forms.

Getting to understand not only the acronyms, but the concepts used in technology, is as essential as knowing how to appropriately file a tax return. Tax is governed by law. As such, it is possible to understand the bells and whistles of any legal provision, and it opens the ability for discussions and gives the ability to resist a government decision, if considered unfair. As Alexis Wichowski explains in her book *The Information Trade*, the net states are imposing their own rules, and there is no easy way for "citizen-users" to claim their rights, as they are corporations used to play by their own rules. Worst, when the net states principles are being implemented by nation-states, the citizens themselves lose their ability to oppose any decision. Their only choice is to follow the rules, and this is how authoritarian regimes are using technology as a powerful support for establishing a more and more absolute power

Good uses of technology

The "net states", i.e. the Big Tech corporations who have gained a level of power and influence at least equal to the "nation states", inherit from the hope that technology will build a "better world", where access to knowledge, providing information immediately at their fingertips, for a small or negligible price, make a positive difference. Being able to be connected constantly can improve and save lives. Technology usage is so pervasive and the rewards are so immediate that no user is willing to go back to a place before technology exists, regardless of its dark side effects.

Nefarious usages of technology

On the contrary, there is a lot that doesn't conform to that model.

It is possible to escape scrutiny and to transfer critical data over national boundaries to protect them

from national laws that are constraining. Digital shelters are used to evade taxes.

The masters of political propaganda have found out that exploiting the borderless connections provided by social media was a powerful way to propagate extravagant rumors, to the effect of weakening trust in democratic institutions including the electoral system in other countries.

The authoritarians or would-be authoritarians have found out that the fine level of control enabled by technologies can be used to serve their purpose of controlling the opinions, and actions of citizens. The smartest ones use the social controls to reward compliant citizens. Instead of punishing the bad citizens, they found it was as efficient to exclude them from social goods or services now reserved to good citizens.

A mixed bag.

We are being told that you can not have the good side without the bad side. If we don't pay to access technology, it's because we accept to be tracked, and our information is valuable and serves the need of an important segment of the economy, allowing companies to target their customers in ways that are unprecedented.

However, things are evolving. We have reached a point where nefarious usages have become serious enough that it carries the dangers of commercial war (between China and the US), civil war (within the US), threatening the survival of democratic societies, free press, free elections, and the rise of authoritarian regimes, partially inheriting from sinister traditions (fascism) but also quite innovative in the ways they have tamed technology usages to serve their needs.

There is no equivalent, on the democratic side, on how technology can serve the needs of the government. Or rather, there are attempts, in various levels of the governments, for example in cities, to try to reverse the trend and use technology to provide better services to the people. But technology remains a black box, that can't be penetrated. For example, campaigns organized by activists or proponents of new groups actively involved in changing things for the better have no problems using Facebook, the same company accused of playing a

role in the demise of democratic values.

In a way, that's normal, as technology is neutral. The fact that we use the letters of the alphabet to communicate ideas, whether considered good or bad, is not held against the fact that we are using words made of letters. The fact that we're using digital information to communicate doesn't mean, similarly, that digital information and its associated technologies is good or bad.

The problem is, therefore, not technology itself. It's the way it is being used, the mechanisms that are at work. As it's easier to analyze how technology is misused than the way it's used, it's interesting to start digging about how technology is used as a political weapon to reach certain goals: political propaganda, fake news, rumors, bullying, human trafficking, tax evasion, money laundering, demeaning democratic values, weakening of institutions, including government.

It is also interesting to analyze which negative feelings are being generated by certain usages of technologies and how these results are achieved. Powerlessness, loss of control, uncertainty, loss of trust, blurring the relation between true and false, impotence, the feeling of overwhelming, impossibility to get a comprehensive picture, inevitability, resignation, deterministic belief that it can't be otherwise.

My hypothesis is that these results, far from being inevitable, are being engineered by people who know what they are doing, and are benefitting from the blindness of the other side, where their opponents are not able to comprehend or devise any strategy to counter it. We will study some of these results and reverse-engineer the way they are produced, in order to give the means to those who want to counter them to address them.

To illustrate those points, it will be useful to pick some examples and dive deeper into the technologies that are used. There is no substitute to not getting into the nitty-gritty parts of the technologies used. Otherwise, things will stay as they are. On the one hand, technologists will continue to work at their micro-level to provide yet more efficient, more scalable, more pervasive, and less accountable technologies, not looking at whether their effects are positive or negative. On the other hand, people who benefit and

people who suffer from the outcomes will continue to witness the growing gap between them.

Less is more, or how big can data grow?

Tracking tech users in a surveillance capitalistic society (S. Zuboff) has assured an unprecedented level of wealth and power to the net states (A. Wichowski) and at the same time has created an unprecedented amount of data to be processed. Technology has followed the trend, and the domain of "big data" has flourished. The results have been quite convincing and machines are now able to provide valuable, and targeted information, to the corporations that need it in order to better target their own customers.

The underestimated side effect of this trend is that the technology used to address smaller amounts of data has lost its appeal, and is considered old-fashioned. But humans are still humans, and the human brain, who remains, if we listen to neurobiologists, far much more sophisticated than any algorithm, tends to be considered inferior to machines, as there is a threshold to the amount of data it can absorb. For example, searching for, let's say, the term "artificial intelligence" in Google, from New York City, on December 11, 2021 at 1:30pm yields "About 767,000,000 results (0.59 seconds)". It's a remarkable achievement that Google is able to produce, in a fraction of a second, three quarters of a billion of hits for that term. But why would I, and any other human being, care about that number?

This sounds ridiculous, but has the effect of showing how short our lifetime is, how limited our brain power, and it leaves us with the impression that although we want to learn something, we'll never be able to get to the bottom of it, nor even scratch the surface. But it shows us also how great Google is, how performant it is, how efficient it is when the goal is to aggregate as much data as possible. In other words, it is self marketing for Google at the detriments of us, poor and powerless human beings.

This rant may end up sounding childish if it was limited to a pure assertion of how great Google is. It does have real world consequences. It encourages some people - inside corporations or governments - to assert that machines are superior to humans, in their efficiency to retrieve and process data. Human expertise is much more expensive (experts went to a long process of education),

is less reliable (experts disagree sometimes), subject to failures (it may be biased), is much slower (it takes more than a fraction of a second for a human to retrieve relevant data on any topic).

And this leads sometimes to the replacement of humans by machines, in the name of progress, like horses have been replaced by cars, or messengers have been replaced by telephones, etc. However, what is absent from the assessment are the same questions that are being raised when dealing with humans. Is it that cheap (search algorithms are not 100% automated, there is a lot of human labor involved in the background)? Is this that reliable? People who create information and know their content often find out that Google fails to report what's most important on their content, because their algorithms are not tailored enough to address their unique content. Then, those who are not the information originators have no way to know how much valuable data they miss. It doesn't matter how many millions or billions of data points there are if the crucial information a user needs is missed. Bias also plays a role, because the results are computed by algorithms that process information according to certain hypotheses. These hypotheses are crafted by human beings, as well. Biases are much aggravated in automated processes. If a wrong, or incomplete, hypothesis has been used, a multiplier effect on the number of data amplified dramatically the effects. Then, like in the human expert case, how do we know if something is right or wrong? It may depend simply on what concepts have been used to calculate it.

Google makes us believe that the rules it applies are transparent by publishing guidelines for search engine optimization. These rules are quite detailed, and a company that wants to comply with us finds itself with procedures that are as arcane and complex than filing financial reports, but depends on Google instead of regulatory procedures created by accountable government bodies. As the search algorithms are kept secret, there is no way to know what other rules Google applies in order to rank search results and have them appear the way they are. A company's success or failure may depend on how it is ranked on search algorithms, and how it compares to its competitors. But there is no way for a company, even less for an individual, to recourse if the outcome is considered unfair.

There are exceptional cases where Google itself modified

its algorithms for a cause they judge morally valid. For example, as Alexis Wichowski points out, searching for ISIS recruitment was diverted to sites that were discouraging it, and leading users to sites providing psychological and emotional support, as Google considered that this could lead to decrease enrollment. And it worked. In this case, the purpose is honorable and can be applauded enthusiastically, but this also shows that Google has the ability to orient the search results to anything it finds valuable at the time. If the winds term, and if these powerful tools fall into the wrong hands, the unattended consequences of such powerful tools is unfathomable. If democratic nation states have no way to weigh in to protect the freedom of expression while prohibiting certain behavior under codified laws, the consequences can be pretty dramatic.

Search engine technologies can be analyzed. The simplest technique is based on "string recognition". Either a word or expression is present or not. Then there are variants of it. Case variations are the simplest. Then there are variations that are more subtle but still useful, such as ignoring accented characters in search. Then there are grammatical variants: plural, conjugated verbs. The technology of natural language processing has been created to handle these cases. Then there is a semantic layer: if a name has synonyms, using either one of the terms could lead to the other. Generalizing this, taxonomies and ontologies have been developed to show each term in relation to others.

If a term has homonyms, then disambiguation techniques can be used. Specific search technologies has been developed for given domains, building on domain-specific vocabularies.

Another aspect of search depends on whether the source data is structured or unstructured. Text is typically unstructured. A database is typically structured. Hybrid, semi-structured data sources are also available. For example, tags marking up text can document the nature of the portion of text within those tags, and therefore end up being equivalent to a structured information source.

All these techniques are used and provide ways for users to define their own research patterns. They can be modified and fine-tuned according to the expected results. Some of them are built on top of proprietary software, others are open-source. Companies provide

domain specific vocabularies or taxonomies that can be applied directly on new information sources.

DuckDuckGo doesn't track users, but is their search engine open source?

Google Search tracks its users, and its search engine is proprietary.

Clueless solutions

Climate Change Data Has Scientists Scrambling for Solutions.

<https://www.wsj.com/articles/climate-change-data-deluge-has-scientists->

Solution found:

"To speed access to the data and lower the cost of computer equipment, NASA and NOAA are working with Amazon Web Services, Google Cloud and Microsoft Corp. to move their climate databases into the cloud."

2 Outperformed by Machines?

Artificial Intelligence / Machine Learning / Internet Of Things

Artificial intelligence is not new. The term was coined in 1956 and has been through several phases of development, with variable success. It has become a buzz word in the recent years and has attracted a lot of traction.

Why is that? The need to analyze enormous amounts of data available has created an incentive for improved automatic processes in order to produce aggregated results, that have a high value for marketing and sales, advertising, political campaigns and all forms of mass media. New techniques have been developed to increase speed and performance: microprocessors continue to be more powerful over time, and on the software side, new techniques are developed to improve performance. Parallel processing is the ability to use multiple computers in order to divide a task into smaller subtasks. Asynchronous programming is the ability to start processing data before all of it is loaded. Various techniques for optimizing data processing continue to be created and implemented. Caching enables to store and reuse data and only update the part of it that has changed.

Data is being analyzed using a variety of techniques, relying on algorithms for optimizing processing speed. An existing term was reused to describe the set of techniques and processes used to that effect: artificial intelligence. The term is somewhat a misnomer, as it is a set of human-created algorithms but the fact that they automate this workflow justifies the term of artificial intelligence. Intelligence in this context is to be understood in the sense of data collection and analysis (as in the Central Intelligence Agency), not directly related to the human feature of intelligence as opposed to stupidity. However, the term is being used as an argument that aims at proving that machines are better than humans as in "artificial intelligence is more powerful than human intelligence", as it handles more data.

Neural networks are built on the metaphor of the computer considered as a human brain. Neural networks are useful, but they pale in comparison with the capabilities of the human brain, especially when applied to the resolution of complex problems.

The research activities in neurobiology using computer models of the human brain still remain at a very early stage and the capacity of the human brain to deal with complex situations is unmatched, and this probably be stay like this for many years to come, despite the spectacular demonstrations of the machine capabilities.

In the general public, unaware of these nuances, the idea that computers are better than humans is making its way. It is clear that automation of repetitive tasks is clearly winning. This affects many more professional sectors than previously thought, including so-called intellectual professions: medical professionals, accountants, lawyers, experts from different fields benefit from help they received from computer-driven systems to collect, sort, organize and present data in ways that were time-consuming and tedious. Low-level tasks, such as boilerplate-based standard legal contracts, diagnosis based on comparing patient data with statistical data, are examples of tasks where automation has clearly benefitted its users, and may have resulted in removing low-level jobs. But the public perception goes broader than that and there is a feeling that many professions are impact, professional careers are threatened, and that the "machines are winning". This results in a loss of purpose, a sentiment that things are now switching to technology-only processes, that without technology nothing is possible. What is being blurred is an understanding of the processes that the machines are better at, some of them having never been done by humans. The notion that machine processing can be seen as a complement to human activity instead of a replacement is very marginal.

Machine Learning and loss of human control

Algorithms which are based on switching on and off zeros and ones at a very high speed, are repetitive. Given the same data set, an algorithm is doing the same thing over and over. There is no surprise to be expected. This is both a good thing and a bad thing. It's a good thing, because algorithms can be used many times, and, when they produce something which is different from what's expected, this often is interpreted as the sign that something is wrong in the algorithm, that there is some bug that needs to be fixed. It's a bad thing, because as data evolves, the algorithms keep repeating over and over the same things. If there is a need to fine tune

manually the results, this task needs to be repeated over and over each time the algorithm is run.

To improve the situation, the idea is to provide a way for the algorithm to analyze the data before it's done, and based on what it has found, modify the end results accordingly. For example, in a search algorithm where many people regularly mistype a word, the spelling error can be recorded and assigned to the proper word, so that the subsequent requests with the ill spelled words would yield the same results as if it would have been typed without the spelling error. This process of enriching the algorithms with more data that improve their efficiency at future runs is called machine learning. Machine learning algorithms are based on mathematical and statistical techniques, which are based on complex processes, and use various models, such as supervised learning and unsupervised learning.

The tools that implement machine learning operate as "black boxes" that take some data as input and produce other data as output. It is not always necessary when implementing a machine-learning engine to master all intermediary steps requiring a deep mathematical and statistical background. For the vast majority of the end users of such products, all these layers are not interesting, or too complex. People tend to rely on the results where they can see visible improvements without having to dig into too many details.

As algorithms can be programmed to modify themselves using these techniques, it comes a point where no human being, including the programmers who started the artificial intelligence project, have the ability to understand what is happening. They are able to tweak slightly the algorithms in the hope to get better results in the cases where it's needed, but it tends to become a guess game, with a whacamole effect. Tweaking algorithms is not easy, as they may produce side effects. The more algorithms are self-correcting, the more difficult it becomes to modify them.

Machine-learning based systems can be a real asset to help digging into huge sets of data, but if they are given the power to take decisions without the ability to check what is happening inside in detail, it can also lead to disastrous consequences in some cases.

The public perception of machine-learning technologies is that humans are becoming more and more irrelevant.

Not only machines do -- or seem to do -- a more efficient jobs than humans, but there is a point beyond which they can't be tamed any more. They have their own logic, and all bets are off.

For those who still consider they are in charge, and are liable for any results that don't fit the expectations, the consequences can be devastating. Before that happens, they understand that they don't have the ability any more to interfere with the technology used. This situation can generate quite an amount of stress, and the sentiment that they lost control.

Losing privacy

Android phones report their location even when they're off (to be checked). For people who are trying to save their freedom to go where they please, and not having to report to any one, this can be a difficult thing to accept. There has been a slow evolution in the renouncement to privacy. Credit cards statements record any purchase we are making, web browsers and cookies leave a trace of our Internet activities, phones track every location we are going. At the same time, the convenience they offer makes it quasi impossible to live without. Not wanting to leave traces is suspicious. For example, trying to buy a plane ticket with cash raises alert levels. Never going on the Internet is in today's world unthinkable in practical terms. There are many services that are not even offered off-line, and it doesn't look like this is going backward.

The most frequent attitude about it is simply to ignore it and not think about it. This is fine as long as we don't do anything that can get us in trouble with the justice system. But in countries where you can be in trouble because of factors that don't depend of what you do, but simply who are: your religion, skin color, income level, social credit score (in China), political opinions (China, Russia, Turkey, etc.), then you can get in real trouble quite soon, with no real way to counter it. It is what is it, and you are left on your own, as in previous 20th century dictatorships, you were constantly followed and all your activities were reported. Your email content is open, the materials you read online, etc., nothing is left in the dark. Freedom and privacy are much more connected than most people think, especially in America where so far the prosecution of people based on their political opinions has been limited, although there have been some dark

periods where personal freedom was at stake.

For those of us who were, directly or indirectly, confronted to political or racial persecution, these restrictions to privacy rights are disheartening. Again, there is a feeling that this goes beyond our control. Regardless how much we pay attention to preserve our individual rights to do whatever we want, we know that we have lost control over it in a significant way.

Technology companies claim that an individual has control about their privacy settings. But the reality is murkier. There are plenty of situations where these settings are ineffective and don't provide real protections. The fine print is where this is hidden, and practically nobody ever reads the terms of service on the Internet. If we would start to read them, it's hard to agree with the majority of them and we wouldn't accept most of them. Not only we lose a big chunk of our individual freedoms, but we feel powerless because there is practically nothing we can do about it. This feeling erodes the trust into a democratic society, which is in principle governed by the will of the people. Where is democracy in an environment where people have lost their ability to express their wills?

So far, hospital patients are being monitored and any indication of a sign going in the wrong direction triggers intervention from a nurse or a doctor. Wearable medical devices, health apps, or even "smart beds" are able to constantly monitor our health condition, and have the potential to save lives by signaling early signs of some vital disfunction. These signals can be sent wirelessly and trigger a quick immediate response. This looks like a good thing to have. But the price to pay is to accept that constant monitoring and therefore lose any sense of privacy, as even in our most intimate places - the bedroom, potentially also the bathroom - data is collected about our gestures, heart beats, and other vital signs.

This is the individual equivalent to the societal change in which societies went through by reinforcing surveillance, therefore limiting freedoms, in the wake of 9/11 terrorist acts. The vaccine mandates are similarly decisions taken by the government to protect the population by imposing constraints on the individual right to choose whether to be vaccinated or not. In order to protect the rights of the unborn, some states decide to prevent women from terminating pregnancies. In

order to protect the life of their citizens, some states have strong restrictions on gun ownership while others have not. Each of these decisions is controversial, and disagreements are based on various perspectives on moral and religious values, the role of government, the balance between individual freedom and the feeling of belonging in a society as a whole. There is no clear-cut answer to any of these questions. A democratic society is characterized by an ongoing public discussion on these issues, and the ability to express opinions, and to regroup with political allies to change things through public debate and voting. A true democratic society is when people have a voice, and the majority of the people can decide. It remains to be seen if the United States, in that respect, still can be counted as a democracy.

Anything made possible by technology is not automatically acceptable without discussion, just because it's possible. When it creates a potential for controversy, it should be submitted to public debates. For example, the ways by which connected products (the Internet of Things) report data should be debatable, and consumers should be fully informed about what a product is capable of reporting before deciding on a purchase. Abuses can result from providing incomplete information. Consumer protection is more and more connected to privacy abuses. It is clear that the price to pay for a democracy to survive is to reign in the surveillance that needs to be accepted through a clear agreement. Having to go through the TSA checks before boarding a plane is clearly a collective decision that depends on the political power and the government. Having one's heartbeats monitored while sleeping should be an individual decision. As the ability to terminate a pregnancy. Vaccine mandates and the right to carry guns is of a different nature, as it endangers not only targeted victims, but also neighbors and bystanders. The parallel with driving is that the mandate to respect traffic lights is of a collective nature, whereas the mandate to fasten one's seatbelt is of an individual nature. However car manufacturers have the obligation to provide cars equipped with seatbelts.

A new right to share should be part of an updated bill of rights. Companies could compete on what they share. If a service is more expensive because it doesn't share, let's be it. Many business offer paid subscriptions with no ads. As data sharing's principal purpose is to serve the advertisement industry, bailing out should be

an option, and many people would gladly pay for it, if offered the option. This extra charge could be called a stamp. The Post office carries letters by requested a fee paid through a stamp. In exchange, the post office guarantees that the mail doesn't get opened. There is no reason why email providers could not guarantee that they are carrying the messages without opening it, even if it goes through a subscription service. Google offers professional email service for a fee, but still reads the content and resells it to its clients.

Inadequate Legal System

The Internet is an open infrastructure, by design. Therefore, restricting its access is very hard, and the basic restrictions are often mere band-aids.

Going on the Internet is like walking on a street. It's very hard to remain anonymous, and not being recognized. We would need to get to ridiculous ways of hiding our face and appearance, to avoid being recognized. Perhaps the combination of a burka, a face mask and sunglasses may prevent others to identify us.

Providing login credentials to enter a private web site is similar to showing an ID when entering a building. It is not 100% secure. It is likely that showing an ID of a person whose photo looks similar to you would get probably get you in most times. Computers are more strict, but bots are able to steal login credentials or in some cases try a multitude of combinations until one works. New protections are working better, such as 2-step identification, including one that sends text messages to your phone. If you do not have your own phone near you, then you can't go further. Of course, this method would not protect you if you lose your phone or it was stolen from you.

Protections are like dams. The DDOS attacks are the equivalent of flooding. The number of requests on a server get so big that the server is not able to offer resistance against the number of simultaneous attacks.

Software has vulnerabilities. Even proprietary software can be hacked, and hackers have developed ways to find those vulnerabilities and to penetrate systems. This is like finding loopholes and using trojan horse tactics. Once you're in, you can go anywhere.

Most users feel they are guilty to not be obedient enough to the most recent rules set to protect them. For example, a 2-step identification is more secure than 1-step. Using a smartphone as a physical device that can only be in the possession of one person at a given time is considered to be a good security measure. If you can prove that you're close to your phone, and you can click "yes" on it, it proves it's you.

Overall, cybersecurity remains an oxymoron. Again, being secure on the Internet is as likely as walking in a street and not being recognized by anyone, including

your next-door neighbor. If you don't want to be seen, don't go out, that will fix it. Moreover, make sure that no recording device is present that could report where you are at a given time. Eventually, this amounts to: if you don't want to be seen on the Internet, don't use any device that is connected to the Internet. That goal, in this day and age, is very hard to achieve.

Private networks, such as Intranet, which are reserved to exclusive use of an organization, use the same techniques than the Internet, but strictly limit access to authorized users. However, this hybrid approach is not entirely secure as it still uses the same technologies and software that the ones that are massively available on the open Internet.

Governments, and organizations which need to ensure full security in their communications, use alternative networks. They are quite exclusive, as they are very expensive to build, operate and maintain. The security challenges they face have more to do with the trust of the people involved. The security protocols under which they operate have to be extremely strict, much stricter than the ones used on the open Internet.

However, on the Internet at least, hackers are getting more and more sophisticated and find creative ways to penetrate servers that are supposedly well protected. In other words, absolute protection is very hard, and the most secure environments are those which are not connected through public networks such as the Internet.

As critical infrastructure depends on Internet-based technologies, vulnerabilities grow and the consequences of the threats can be deadly. Cyberwar is not any more in the domain of science fiction. It is as concerning today, than the danger of nuclear was in the late 1950s.

Everybody can publish

Publishing on the Internet is very easy thanks to social media platforms. The rules for publishing are much looser than the ones that are needed to publish print materials. With print, one needs to create, print, and distribute using heavy technologies such as printing presses and efficient distribution channels. With an account on a social media platform, within a few minutes it is possible to become a publisher.

Freedom of speech is protected by the first amendment

right, and equivalent rules and statutes in democratic societies. In not-so-democratic societies, rules are more stringent. Publishers have some responsibilities and duties and are liable for their content. Some legal provisions enable those who feel their integrity or reputation have been attacked to sue publishers. The rules against abuses committed by individuals publishing online on privately owned platforms are murkier. Bullying, propagation of false rumors and fake news, is therefore much easier. As publishing platforms are looking for content that keep their audience riveted, they are less likely to stop outrageous content. In the printed press world, we know what to expect when reading a tabloid. If we are not interested by this type of content, we can choose to read a more serious newspaper. Reputations are at the publication level, because for every publication, the publisher takes responsibility over its content. On social media platforms, all content is published in a uniform form, there is no decentralized distribution of editorial responsibility, and anything goes, without the ability to distinguish clearly what is based on proven facts from what is based on political propaganda or false rumors.

Once any data is published, it is very hard to "unpublish", i.e. to remove it from public view. It's as complex as trying to get the toothpaste back in the tube. This can be very distressing if an unauthorized picture or video is published accidentally or by another person in an act of malfeasance. There are many stories of young people being bullied online, with tragic consequences.

Cryptocurrencies

Cryptocurrencies have been designed to circumvent the traditional financial system, and can be used both to facilitate money exchanges worldwide, for good or bad purposes.

Cybercrimes are on the rise, and are using several loopholes made available by the creation of cryptocurrencies.

Losing control over legislation and distribution of information

The provisions of the existing legal systems are not adapted to the online world:

- national laws can be circumvented by the borderless, world-wide circulation of information over the Internet.

- in federated countries, such as the USA, the state-based commerce laws are not adapted to the interstate provision of services enabled by the Internet. Any product that is available online is subject to interstate commerce, and this makes the handling of commercial laws very hard to abide to.

- social media platforms publish content without bearing direct responsibility for the quality of the content. Therefore they are less accountable than traditional publishers, and their liabilities are dissolved. The broadband companies, on the other hand, influence content as they attempt to remove the net neutrality features. It's similar as if a train or truck company would decide to privilege who gets to be privileged in receiving printed materials depending on how influential the receivers are. This leaves us in a pickle, as a society.

Losing Control and Initiative at Work

Computers are everywhere. For many people working means operating software on a computer, collecting and analyzing data, producing new data, communicating information, etc. That goes beyond traditional white collar occupations, as manual workers also use tablets or digital devices on their workplace.

Overall, digitization means that work is easier. Repetitive tasks are less frequent, overall organization is more rationalized, and working conditions have improved.

However, some drawbacks have also started to emerge. Because workflows are digitized, they therefore can't be easily modified without interfering with the software. This can lead to more rigidity, or sometimes the mere impossibility to resolve a problem because "the computer system won't let us do it."

Many issues have to do with customer support. First, the voice mail systems are often irritating, because they are designed to give the illusion that we are talking to a person, whereas we are talking to a computer. The number of options is limited, it often doesn't include the exact question we need an answer to. And if the computer doesn't understand the question, it keeps repeating over and over the same thing. As the computer speaks with a human voice, it's like talking to a person who is really really stupid. Not only customers don't get what they are looking for, but it gives a bad reputation to the company that seems not to care about their satisfaction.

Once we get over this first obstacle, and we are able to speak with a human being, we may end up explaining the problem, and getting the answer: I understand your concern, but our computer system doesn't allow us to do what you want. If it were me, I would have done it, but I can't.

There we have an admission, that working people have lost control over the ability to take decisions because they are subject to rules that depend on the technology and on which they have no weight. They have lost control over what they can do, and they accept it as something inevitable. They expect the caller to understand it -- implicitly recognizing that we are all in the same boat,

subject to the powers of an unreachable, higher level, technology under.

They could have given a different answer: we understand that currently our computer system doesn't allow us to do what you need. We will work on it to ensure that in the future your expectations will be met. In doing so, they would recognize that technology is evolving, that users have their word in how it evolves.

But the fact that it's not happening is because end users (here the company providing services to their customers) have lost hope that they can do something. There is an invisible glass ceiling which is considered unbreakable, and that amounts to consider that anything technical is out of reach.

Technology is complex. Naïve and uneducated users think they can do what they consider simple things with computers, only to discover soon enough that they don't get what they are asking for. There are many layers involved, they keep evolving, and just making something work at all is extremely challenging. This explains why the software industry is getting more and more concentrated into the hands of a smaller number of companies.

More experienced users are painfully aware that they won't get everything they want, and whether they have unsuccessfully tried or not, they realized that they are better off adjusting to what they get rather than asking for something that doesn't exist, even if this is what they would want. Ironically, "what you see is what you get" (WYSIWYG) was the way to sell progress in the 1980s showing that a page could be tailored at will before getting printed. Now the same expression can still be used and understood as: "if you don't see it, you don't get it"!

More than one paradigm

Big data rules the world. That proposition holds for advertising. In order to find where your customers are, it's convenient to analyze as many data points as possible, run all possible filters to target a precise segment of the market, so that you can get the result you need.

Big data needs have generated big data technologies. Algorithms have been adjusted to scale up, optimization

techniques are applied to accelerate the production of results. The mere size of the data available has generated a set of new tools, techniques, and technologies, that are able to produce impressive results handling an impressive amount of data.

Because of the importance of that market sector, a lot of investment has been made in this domain, and the Big Tech companies have created unique technologies that are used to this goal. And because of all this accumulated trove, they have been eager to reuse the same tools and techniques all over, and have propagated the idea that using technology means using big data technology. For example, the job interviews for tech jobs are based on "data structures" and "algorithms" created for this big data ecosystem.

However, this obfuscates the fact that many technology users are dealing with data sets that are much smaller (even if at their scale it seems big). For example, a government agency produces data, that is reasonably large, but would consider to be ridiculously small compared to the scale of big data. Instead of tera- or peta-bytes of data (big) we are talking here of a few hundred thousand of data points. Although this seems overwhelmingly large, it is small compared to the scale of big data.

Any technology is not always the best choice at any scale. The "small data" world has several distinctive characteristics that differ from the "big data" world. The biggest difference is that in big data, nobody is interested to look at individual data points, other than at an aggregation of data points considered at a statistical level. In small data, for example in a government agency, it is possible to find who has created a subset of this data, and ask them why these data points have been designed the way they were. If there are adjustments to be made, it is possible to discuss them. Also, there is a requirement for an agency to disseminate information which is entirely reliable, meaning not just 95% correct, but should be as close as possible to 100% correct. The reason for that is that the people who created, and/or published that information are accountable, they bear the responsibility to get information that can be considered as an authoritative reference in the matter, and therefore have no choice but have to ensure that their information is entirely dependable.

These are two completely different use cases, and it should come to no surprise that the kinds of technologies to produce data in either case should be different. The reality is that they are not so much different. The weight of the big tech companies involved in big data software and services is so disproportionately high that they make everybody believe that their solutions can be applied even when they obviously would not, if we think just a little bit about it. But thinking about it is not what people are used to, unfortunately.

Losing Control

Not only people lose control about what they can do to better serve their own needs, but they also lose control about what tools they use in order to satisfy their requirements. Often, they don't even know that alternatives are envisionable, and they are resigned to the idea to what they are looking for is unrealistic. This creates a feeling of passivity and uselessness. If they know that other solutions exist but can't get them, it created a feeling of frustration and powerlessness.

Either way, the outcome is not great!

5 Can't compete against Big Tech monopolies

5- Losing Control inside Tech: Amazon vs. Elastic Search
. Technology evolves rapidly. Graphic Design vs. User Experience vs. Javascript. Engineering, Open Source, Hacking, Code of Conduct. Inadequate Job Hiring profiles
. Role of algorithms and data structures. No No No: NoCode, NoSQL. The Language War/ Operating System War. Is it still relevant? - Tableau, Miro, Airtable, Notion, Zoom, etc. The new business models. Where have IBM and Microsoft gone? Platforms. Frontend, Databases, Frameworks. The role of Facebook, Google, Twitter, Uber

Brief history

Today's technology can be divided into three main subdomains: devices, networks and platforms. When personal computers were first released, they were productivity tools aiming at providing better ways to perform office work.

In order to better understand technology, lets divide it into several domains.

- Devices: Computers, tablets, phones, IOTs, watches, glasses, digital assistants. They provide connection to the Internet.
- Networks: Broadband, Servers, Internet, World-Wide Web, Intranet, Cloud, Private Virtual Network. Orchestration, Automation, Servers.
- Platforms, Software, Operating Systems, Languages and Ecosystems: Facebook (including Instagram and WhatsApp), Google (including Android and YouTube), Amazon, Microsoft (including Windows, Skype, LinkedIn), Twitter, Zoom, Uber, AirBnB, Apple (IOS, MacOS), Open Source, Oracle

1980s: Computers become personal

- Main players: IBM and Microsoft
- Important outsider: Apple

1990s: WWW

- Silicon Valley is the center of the world.
- New disruptive technology about the change the world.
- Online Media and E-Commerce

2000s: Collecting data for the advertisement industry

- Google does garbage collection and finds treasures, that they can sell.
- Facebook baits people into connecting with each other and sells their data
- Big data starts.

2010s: Smartphones + Cloud + Bad actors enter into play

- The whole world gets digitized through smartphones.
- Industrial Concentration in the US, unregulated.
- Russians see tech as an easy way to extend their influence into propaganda
- China expands its role in producing tech, and transforms its society into tech-driven dictatorship

Technological evolutions

- Predominance of big data technologies.
- How big tech open-sources part of their technologies to create satellites. Google-> Angular + Material, Facebook -> React, Twitter -> Bootstrap, Uber -> Vis, etc.
- Government and universities get on dead ends: The graveyard of good will thinking: Upper-level ontologies, taxonomies, Semantic Web, XML, etc.
- The complexification and multiple divisions of technological layers
- Big eats Small: Amazon vs. ElasticSearch, etc.
- The big tech propaganda main lines.
- Evolution of software trends:
 - Databases. SQL / NoSQL with query languages.
- Resilience / Resistance?
 - The Hacker Community, Open-Source, Public-Interest Tech, City-supported tech (NYC), etc.
 - Independent frameworks: E.g. Vue
 - New Programming Languages and Paradigms.

Control Lost:

- Impossible to function without a smartphone. Too many services have become indispensable.
- Impossible to develop software without the cloud: operating-systems based systems are decaying. A computer

becomes (again) a terminal. Impossible to disconnect from the web.

Chapter 6.

US losing lead in technology

Concentration

Tech is a huge economic sector that employs lots of people worldwide. That includes the production of devices, software, networks, applications, content, marketing.

The software industry has undergone a massive transformation during the last 10 years. Migration of data and software to cloud-based servers has been massive. The amount of data created and exchanged has grown astronomically and the growth is expected to continue.

The technology industry has undergone concentration. Production of raw materials and devices is now centered in Far-East Asia (mainly in China), the companies that provide cloud-services and infrastructures is a handful, as well as companies that provide services to deal with content, whether social media, or Internet-wide data analysis.

The industrial concentration has been possible by a combination of factors. The understanding that aggregating user data without them interfering with the process has created a trove of incredibly valuable data that could be sold without major obstacles.

The understanding (Karl Marx) that owning the means of production means power has driven China to control the supply of the devices used in the industry worldwide and has given China an unsurpassed domination role in the world.

Net states vs. Nation-states

Tech companies have accumulated an enormous amount of power in the democratic countries (mostly in the US) and have become as powerful (sometimes more) than nation states (see Wichowski).

Democracy is under attack by authoritarians who are either user tech to their advantage, or are claiming that tech inevitably look to authoritarian societies (follow the guide, whether it's a tech user guide or a nation's Führer).

Citizen-users have become passive, resigned, powerless , and have lost hope that things can improve.

Silicon Valley has stopped to be an innovation engine

Back in the 1990s, the Silicon Valley was in ebullition.

The advent of the World-Wide Web was going to change the world for the better, disrupt most of human activities. Since then, disruption has happened, things have been disrupted. Lots of good things have happened (as forecast) but also lots of bad things have happened (first dismissed as marginal, then increasingly visible).

Big Tech has concentrated the intellectual and innovative workforce. Innovations are now limited to what serves their business model. Other forms of innovative thinking, especially if they result in making their business model in danger, are ignored, or killed. Universities and public research on technology is not on par with big tech research departments. Big Tech uses academic institutions to recruit for themselves, and have a paternalistic, "charity-like" condescending behavior. They know they can't be beaten at the technical levels, because they hold the keys to the complex layers of technology involved. The cost of entry into tech-based research has dramatically increased.

Smart authoritarian regimes have understood the benefit they can derive from this situation. China has found ways to support and lead innovation to their interest as a country, get international recognition, by submitting tech companies to their objectives. Companies follow government orders in China, not the reverse.

In the meantime, in the US, the tech companies held the government hostage. They ridicule the Congress ignorance during hearings where they are supposed to be grilled on their abusive monopoly power, and end up revealing how inept and ineffective these attempts are. According to S. Zuboff, deals about surveillance between the government and data collecting companies ensure the government to get access to information they need (for example to hunt terrorists, or to get accurate information about the electorate) while leaving empty

any constraints of regulating the surveillance power of tech giants. Absence of accountability on both sides results in not only weakening of the power of democracy, but preventing real competition as a basis in a free-market capitalist society, and kills innovation coming from the United States. Added to a restrictive immigration policy (which also has the effect of attracting foreign students, training them, and then not allowing them to stay), the US is unwillingly accelerating its demise as a world leading force in technology advancement.

Towards an NIT

An unfulfilled need.

Social media platforms have become immensely influential ; computers process unprecedented amounts of data; and the increasing complexity of Information Technology is getting more and more complex, and follows its own rules and structures that are impenetrable to most everyone.

Big Tech companies and potential bad actors in government have little accountability when deploying such systems—in light of secret, proprietary algorithms. Similarly, heavy-handed (let alone authoritarian) governments can exploit these technologies to blur the differences between truths and falsehoods. Russia and China are examples—even to the extent of interfering in democratic elections overseas.

A democratic society such as the US needs to have a clearer vision of how it can tame technological evolution to simultaneously foster innovation and preserve the rights of its citizens against authoritarianism, abusive attacks against privacies, monopolies, etc.

A precedent: NIH

- The National Institute of Health provides leading-edge research and is considered the best medical research center world-wide. Not only it develops its own research and product activities, but is the source of funding for the domain of biological and medical research for academic and private-based research activities. It works in close contact with the agencies such as CDC, FDA that regulate the market, authorize new products.

The tension between net states and the US nation state

- Non-ingerence deals (see Zuboff on Google with CIA after 9/11 and Google and the Obama Campaign)

The political need for digital literacy

- The congressional hearings with Zuckerberg were not only ridiculous, they are outrageous.
- Breaking monopolies is not the appropriate answer to nation-state vs. net state
- Democracy needs to be preserved. The nation-state can't dictate everything.
- Big Tech corporations should be regulated.
- New laws should be created to preserve individual

freedoms.

The need to design nation-wide tech projects

- The nation-state can become a competitor against big tech, for example by providing a mail service that respects privacies. A national email service could be created based on the post office mail system, i.e. that respects privacy: as letters are not opened by the Post office, a national email service could guarantee that the contents of the email can be confidential. Only judicially-permitted investigations would justify to open the mail by law. In other words, any law-abiding citizen would be able to exchange email privately.

- A public search engine could provide access to knowledge without being tracked. Public libraries traditionally preserve the right to their patrons to read any books without recording what they read. The current universal tracking system doesn't protect the right to access information needed. For example, it is currently risky for anybody to find information about terrorism, even if the only goal is to understand how it works, where it comes from, in order to be better informed. Searching for information about terrorism carries the risk to be flagged as a would-be terrorist.

- A public social media could be created, that would have the ability to connect people together and would do that explicitly without tracking. This would foster communication between people without them being inundated with ads. This public social media network should be well protected to preserve it to being surveilled either for marketing or political purposes. Abuses should be monitored, and new laws should be created to prevent it from happening, and give a recourse to citizens who claim that their privacy rights have been infringed.

- Voting machines should have their software being disclosed as open source, allowing tech savvy citizens to analyze them, find potential bugs and loopholes, and there should be an open discussion about their maintenance. Only this publicly available software should be authorized in any machine that is being used for voting, at any governmental level: federal, state, municipal. This would go a long way to restore public confidence in the electoral system.

- New legal provisions should be studied and

experimented to provide a publishing system adequate to the digital age. Publishers should be able to publish freely, in accordance to the First Amendment, with some possible limitations regarding hate crime, support for violent actions. Publishers, including individuals publishing on social media, should comply with those provisions and should be held liable in case of violations. This model should be created by looking at the best practices from the news, media, and book publishing worlds in a democratic society. Publication of information with detrimental effects, for example harrasment and bullying, should be compared against existing libel laws. New specific laws should be enacted , and find the balance between freedom of speech and respect of individual rights and reputation. In any case , the level of responsibility should be possible to establish. Broadband service providers, social media platforms, and creators of the information should have their responsibilities defined with the existing, or new , legal provisions.

- Secure cloud services and storage could be provided that would prevent any abuse, such as the Amazon vs. ElasticSearch story, in which Amazon, who is the cloud providers, has "stolen" the information stored by ElasticSearch and has created a competing technology that has jeopardized the commercial success of its client. Again, government-supported cloud service should guarantee that the information remains well protected. Obviously, the terms of service should prevent all kinds of nefarious data to be stored on those services.

- Research on accountability of information systems. This not only affects the financial sector, with projects involving cryptocurrencies and BlockChain, but also research on designing ways to dig into artificial intelligence and machine learning algorithms and reverse engineer some of the processes in order to demystify the magic that these systems have, with possibly negative consequences. More specifically, the ability to understand and investigate how these systems work could be of great benefit for many.

- A secondary benefit is that once the government is able to create its own, technologically advanced products, it will make it easier to trick down this information to Congress and all elected officials and get them a much more precise knowledge of what technology is, where it is heading, and what they can do

about it.

- It happens that benefits of technological advances are for some time disconnected from short term profits. The investor-based model driving the funding of the start-up ecosystem is looking for immediate returns of investment, therefore does not support any project that is incapable of showing them. The intense research activities inside big tech corporations is aimed at reinforcing their business models, and therefore neglects other projects that don't fall into that framework. Therefore, there are a lot of projects that don't get funded, that could lead to breakthroughs in the future. Only government-funded research could fulfill that need. It is essential for US competitiveness in the world that it stays on top of the technology advances, because the current trend is that the authoritarian regimes are getting a solid grip on technological advances while democratic societies are letting the private sector lead and are taken aback consequently, as they lose control over the directions in which technology is heading.

- Some public-interest projects could reverberate worldwide and restore American influence. For example, if some technological breakthroughs can be used for better monitoring climate change, reduce inequities, and increase the general public literacy towards technology, there will be incentives to export this knowledge to other countries and foster cooperation, education, etc.